ABSTRACT

The invention relates to a cryptographic method wherein a random number generator producing random numbers S_i whose size N is fixed between 0 and W-1 is used to produce a random number R between 0 and a predefined limiter K. According to the invention: E31: a random variable S_i is produced, ranging from 0-W-1, E32: if the random variable S_i is strictly lower than a coefficient K_i of the limiter K in base W, the coefficient R_i of order i of the random number R is equal to the random number S_i then, for all orders j which are lower than i, a random variable S_j of 0-W-1 is produced and $R_j=S_j$. E33: unless, if said random variable is greater than coefficient K_i of position i of the limiter K is base W, whereupon said coefficient R_i is determined on the basis of the random variable Si of order i according to a predetermined function, then a coefficient R_{i-1} is determined for the random number R of order i-1 which is immediately lower by repeating stages E31 - E33. The invention also relates to an electronic component which is adapted for implementation of said method and a chip card with said component integrated therein. The invention can be applied to cryptographic calculation.